

GAO

Report to the Acting Commissioner of
Internal Revenue

January 2008

**INFORMATION
SECURITY**

**IRS Needs to Address
Pervasive Weaknesses**





Highlights of [GAO-08-211](#), a report to the Acting Commissioner of Internal Revenue

Why GAO Did This Study

The Internal Revenue Service (IRS) relies extensively on computerized systems to carry out its demanding responsibilities to collect taxes (about \$2.7 trillion in fiscal year 2007), process tax returns, and enforce the nation's tax laws. Effective information security controls are essential to ensuring that financial and taxpayer information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of its audit of IRS's fiscal years 2007 and 2006 financial statements, GAO assessed (1) IRS's actions to correct previously reported information security weaknesses and (2) whether controls were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. To do this, GAO examined IRS information security policies and procedures, guidance, security plans, reports, and other documents; tested controls over key financial applications at three IRS data centers; and interviewed key security representatives and management officials.

What GAO Recommends

GAO is recommending that the Acting Commissioner take several actions to fully implement an agencywide information security program. In commenting on a draft of this report, IRS agreed to develop a detailed corrective action plan addressing each of the recommendations.

To view the full product, including the scope and methodology, click on [GAO-08-211](#). For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Nancy Kingsbury at (202) 512-2700 or kingsburyn@gao.gov.

INFORMATION SECURITY

IRS Needs to Address Pervasive Weaknesses

What GAO Found

IRS made limited progress toward correcting previously reported information security weaknesses. It has corrected or mitigated 29 of the 98 information security weaknesses that GAO reported as unresolved at the time of its last review. For example, IRS implemented controls for user IDs for certain critical servers, improved physical protection for its procurement system, developed a security plan for a key financial system, and upgraded servers that had been using obsolete operating systems. In addition, IRS established enterprise-wide objectives for improving information security, including initiatives for protecting and encrypting data, securing information technology assets, and building security into new applications. However, about 70 percent of the previously identified information security weaknesses remain unresolved. For example, IRS continues to, among other things, use passwords that are not complex, grant excessive access to individuals who do not need it, and install patches in an untimely manner.

In addition to this limited progress, other significant weaknesses in various controls continue to threaten the confidentiality and availability of IRS's financial processing systems and information, and limit assurance of the integrity and reliability of its financial and taxpayer information. IRS has not consistently implemented effective controls to prevent, limit, or detect unauthorized access to computing resources from within its internal network. For example, IRS did not always (1) enforce strong password management for properly identifying and authenticating users, (2) authorize user access to only permit access needed to perform job functions, (3) encrypt sensitive data, (4) effectively monitor changes on its mainframe, and (5) physically protect its computer resources. In addition, IRS faces risks to its financial and taxpayer information due to weaknesses in implementing its configuration management policies, as well as appropriately segregating incompatible job duties. Accordingly, GAO has reported a material weakness in IRS's internal controls over its financial and tax processing systems. A key reason for the weaknesses is that the agency has not yet fully implemented its agencywide information security program to ensure that controls are effectively established and maintained. As a result, IRS is at increased risk of unauthorized disclosure, modification, or destruction of financial and taxpayer information.

Contents

Letter		1
	Results in Brief	2
	Background	3
	Objectives, Scope, and Methodology	6
	IRS Has Made Limited Progress in Correcting Previously Reported Weaknesses	8
	Significant Weaknesses Continue to Place Financial and Taxpayer Information at Risk	9
	Conclusions	21
	Recommendations for Executive Action	22
	Agency Comments	22
Appendix I	Comments from the Internal Revenue Service	25
Appendix II	GAO Contacts and Staff Acknowledgments	27

Abbreviations

CIO	chief information officer
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
MA&SS	Mission Assurance and Security Services
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TIGTA	Treasury Inspector General for Tax Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

January 8, 2008

The Honorable Linda E. Stiff
Acting Commissioner of Internal Revenue

Dear Ms. Stiff:

The Internal Revenue Service (IRS) has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. It relies extensively on computerized systems to support its financial and mission-related operations. Effective information system controls are essential to ensuring that financial and taxpayer information are adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. These controls also affect the confidentiality, integrity, and availability of financial and sensitive taxpayer information.

As part of our audit of IRS's fiscal years 2007 and 2006 financial statements,¹ we assessed the effectiveness of the service's information security controls² over key financial systems, information, and interconnected networks at three locations. These systems support the processing, storage, and transmission of financial and sensitive taxpayer information. In our report on IRS's fiscal years 2007 and 2006 financial statements, we reported that the new information security deficiencies we identified in fiscal year 2007 and the unresolved deficiencies from prior audits represent a material weakness³ in internal controls over financial and tax processing systems.

¹GAO, *Financial Audit: IRS's Fiscal Years 2007 and 2006 Financial Statements*, [GAO-08-166](#) (Washington, D.C.: Nov. 9, 2007).

²Information security controls include logical and physical access controls, configuration management, segregation of duties, and continuity of operations. These controls are designed to ensure that access to data is appropriately restricted, that physical access to sensitive computing resources and facilities is protected, that only authorized changes to computer programs are made, that computer security duties are segregated, and that back-up and recovery plans are adequate to ensure the continuity of essential operations.

³A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

We assessed (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses and (2) whether controls over key financial and tax processing systems are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. We performed the above audit work from April 2007 through October 2007 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

IRS made limited progress toward correcting previously reported information security weaknesses. It has corrected or mitigated 29 of the 98 information security weaknesses that we reported as unresolved at the time of our last review. For example, IRS implemented controls for user IDs for certain critical servers, improved physical protection for its procurement system, developed a security plan for a key financial system, and upgraded servers that had been using obsolete operating systems. In addition, IRS established enterprisewide objectives for improving information security, including initiatives for protecting and encrypting data, securing information technology assets, and building security into new applications. However, about 70 percent of the previously identified information security weaknesses remain unresolved. For example, IRS continues to, among other things, use passwords that are not complex, grant excessive access to individuals who do not need it, and install patches in an untimely manner.

In addition to this limited progress, other significant weaknesses in controls intended to restrict access to data and systems, as well as other information security controls, continue to threaten the confidentiality and availability of its financial and tax processing systems and information, and limit assurance of the integrity and reliability of its financial and taxpayer information. IRS has not consistently implemented effective controls to prevent, limit, or detect unauthorized access to computing resources from within its internal network. For example, IRS did not always (1) enforce strong password management for properly identifying and authenticating users, (2) authorize user access to permit only the access needed to perform job functions, (3) encrypt sensitive data, (4) effectively monitor changes on its mainframe, and (5) physically protect its computer resources. In addition, IRS faces risks to its financial and taxpayer information due to weaknesses in implementing its

configuration management policies, as well as appropriately segregating incompatible job duties. A key reason for these weaknesses is that IRS has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. Until these weaknesses are corrected, the agency remains particularly vulnerable to insider threats. As a result, IRS is at increased risk of unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as inadvertent or deliberate disruption of system operations and services. Further, IRS will not have assurance that the proper resources are applied to known vulnerabilities or that those vulnerabilities will be properly mitigated.

We are making recommendations to the Acting Commissioner of Internal Revenue to take several actions to fully implement a comprehensive, agencywide information security program. We also are making recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses related to identification and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, and segregation of duties.

In providing written comments on a draft of this report, the Acting Commissioner of Internal Revenue recognized that there is significant work to be accomplished to address IRS's information security deficiencies, and stated that the agency is taking aggressive steps to correct previously reported weaknesses and improve its overall information security program. She further stated that IRS would develop a detailed corrective action plan addressing each of our recommendations.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have revolutionized the way our government, our nation, and much of the world communicate and conduct business. Although this expansion has created many benefits for agencies such as IRS in achieving their missions and providing information to the public, it also exposes federal networks and systems to various threats. The Federal Bureau of Investigation has identified multiple sources of threats, including foreign nation states engaged in information warfare, domestic criminals, hackers, virus writers, and disgruntled employees or contractors working within an

organization. In addition, the U.S. Secret Service and the CERT Coordination Center⁴ studied insider threats, and stated in a May 2005 report that “insiders pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases.”

Without proper safeguards, systems are unprotected from individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. These concerns are well founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. For example, the Office of Management and Budget (OMB) cited⁵ a total of 5,146 incidents reported to the U.S. Computer Emergency Readiness Team (US-CERT)⁶ by federal agencies during fiscal year 2006, an increase of 44 percent from the previous fiscal year.

Our previous reports, and those by inspectors general, describe persistent information security weaknesses that place federal agencies, including IRS, at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, we have designated information security as a governmentwide high-risk area since 1997,⁷ a designation that remains in force today.⁸ Recognizing the importance of securing federal agencies’ information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002⁹ to strengthen the security of information and systems within federal agencies. FISMA requires each

⁴The CERT Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

⁵OMB, *FY 2006 Report to Congress on Implementation of the Federal Information Security Management Act of 2002* (Washington, D.C., March 2007).

⁶US-CERT’s mission is to protect the nation’s Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks by analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

⁷GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997).

⁸GAO, *High-Risk Series: An Update*, [GAO-07-310](#) (Washington, D.C.: January 2007).

⁹FISMA was enacted as title III, E-Government Act of 2002, Pub L. No. 107-347, 116 Stat. 2946 (Dec. 17, 2002).

agency to develop, document, and implement an agencywide information security program for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management. Such a program includes developing and implementing security plans, policies, and procedures; testing and evaluating the effectiveness of controls; assessing risk; providing specialized training; planning, implementing, evaluating, and documenting remedial action to address information security deficiencies; and ensuring continuity of operations.

IRS has demanding responsibilities in collecting taxes, processing tax returns, and enforcing the nation's tax laws, and relies extensively on computerized systems to support its financial and mission-related operations. In fiscal years 2007 and 2006, IRS collected about \$2.7 trillion and \$2.5 trillion, respectively, in tax payments; processed hundreds of millions of tax and information returns; and paid about \$292 billion and \$277 billion, respectively, in refunds to taxpayers. Further, the size and complexity of IRS adds unique operational challenges. The agency employs tens of thousands of people in 10 service center campuses, 3 computing centers, and numerous other field offices throughout the United States.

IRS also collects and maintains a significant amount of personal and financial information on each American taxpayer. The confidentiality of this sensitive information must be protected; otherwise, taxpayers could be exposed to loss of privacy and to financial loss and damages resulting from identity theft or other financial crimes.

The Commissioner of Internal Revenue has overall responsibility for ensuring the confidentiality, integrity, and availability of the information and information systems that support the agency and its operations. FISMA requires the chief information officers (CIO) at federal agencies to be responsible for developing and maintaining an information security program. Within IRS, this responsibility is delegated to the Chief of Mission Assurance and Security Services (MA&SS). The Chief of MA&SS is responsible for developing policies and procedures regarding information technology security; establishing a security awareness and training program; conducting security audits; coordinating the implementation of logical access controls into IRS systems and applications; providing physical and personnel security; and, among other things, monitoring IRS security activities. To help accomplish these goals, MA&SS has developed and published information security policies, guidelines, standards, and procedures in the *Internal Revenue Manual*, the *Law Enforcement*

Manual, and other documents. The Modernization and Information Technology Services organization, led by the CIO, is responsible for developing security controls for systems and applications; conducting annual tests of systems; implementing, testing, and validating the effectiveness of remedial actions; ensuring that continuity of operations requirements are addressed for all applications and systems it owns; and mitigating technical vulnerabilities and validating the mitigation strategy. In July 2007, IRS began undergoing an organizational realignment that dissolved MA&SS and moved responsibilities for managing the servicewide information security program to a newly created position—the Associate CIO for Cybersecurity.

Objectives, Scope, and Methodology

The objectives of our review were to determine (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses and (2) whether controls over key financial and tax processing systems were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. This review was performed in connection with our audit of IRS's financial statements for the purpose of supporting our opinion on internal controls over the preparation of those statements.

To determine the status of IRS's actions to correct or mitigate previously reported information security weaknesses, we identified and reviewed its information security policies, procedures, practices, and guidance. We reviewed prior GAO reports to identify previously reported weaknesses and examined IRS's corrective action plans to determine for which weaknesses IRS reported corrective actions as being completed. For those instances where IRS reported it had completed corrective actions, we assessed the effectiveness of those actions. We evaluated IRS's implementation of these corrective actions for two data centers, and one additional facility.

To determine whether controls over key financial and tax processing systems were effective, we tested the effectiveness of information security controls at three data centers. We concentrated our evaluation primarily on threats emanating from sources internal to IRS's computer networks and focused on three critical applications and their general support systems that directly or indirectly support the processing of material transactions that are reflected in the agency's financial statements. Our evaluation was based on our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information system

controls that affect the confidentiality, integrity, and availability of computerized information.

Using National Institute of Standards and Technology (NIST) standards and guidance, and IRS's policies, procedures, practices, and standards, we evaluated controls by

- testing the complexity and expiration of passwords on servers to determine if strong password management was enforced;
- analyzing users' system authorizations to determine whether they had more permissions than necessary to perform their assigned functions;
- observing data transmissions across the network to determine whether sensitive data were being encrypted;
- observing whether system security software was logging successful system changes;
- testing and observing physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;
- inspecting key servers and workstations to determine whether critical patches had been installed or were up-to-date; and
- examining access responsibilities to determine whether incompatible functions were segregated among different individuals.

Using the requirements identified by FISMA, which establish key elements for an effective agencywide information security program, we evaluated IRS's implementation of its security program by

- analyzing IRS's risk assessment process and risk assessments for key IRS systems to determine whether risks and threats were documented;
- analyzing IRS's policies, procedures, practices, and standards to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;
- analyzing security plans to determine if management, operational, and technical controls were in place or planned and that security plans were updated;

-
- examining training records for personnel with significant responsibilities to determine if they received training commensurate with those responsibilities;
 - analyzing test plans and test results for key IRS systems to determine whether management, operational, and technical controls were tested at least annually and based on risk;
 - observing IRS's process to correct weaknesses and determining whether remedial action plans complied with federal guidance; and
 - examining contingency plans for key IRS systems to determine whether those plans had been tested or updated.

We also reviewed or analyzed previous reports from the Treasury Inspector General for Tax Administration (TIGTA) and GAO; and discussed with key security representatives and management officials whether information security controls were in place, adequately designed, and operating effectively.

IRS Has Made Limited Progress in Correcting Previously Reported Weaknesses

IRS has made limited progress toward correcting previously reported information security weaknesses. It has corrected or mitigated 29 of the 98 information security weaknesses that we reported as unresolved at the time of our last review. IRS corrected weaknesses related to access controls and personnel security, among others. For example, it has

- implemented controls for user IDs for certain critical servers by assigning each user a unique logon account and password and removing unneeded accounts (guest-level);
- improved physical protection for its procurement system by limiting computer room access to only those individuals needing it to perform their duties;
- developed a security plan for a key financial system; and
- updated servers that had been running unsupportable operating systems.

In addition, IRS has made progress in improving its information security program. For example, the agency is in the process of completing an organizational realignment and has several initiatives underway that are designed to improve information security such as forming councils and

committees to foster coordination and collaboration on information technology security policies, procedures, and practices. IRS also has established six enterprisewide objectives for improving information security, including initiatives for protecting and encrypting data, securing information technology assets, and building security into new applications.

Although IRS has moved to correct previously identified security weaknesses, 69 of them—or about 70 percent—remain open or unmitigated. For example, IRS continues to, among other things,

- use passwords that are not complex,
- grant excessive electronic access to individuals not warranting such access,
- allow sensitive data to cross its internal network unencrypted,
- allow changes to occur on the mainframe that are not properly monitored or recorded,
- ineffectively remove physical access authorizations into sensitive areas,
- install patches in an untimely manner, and
- improperly segregate incompatible duties.

Such weaknesses increase the risk of compromise of critical IRS systems and information.

Significant Weaknesses Continue to Place Financial and Taxpayer Information at Risk

In addition to this limited progress, other significant weaknesses in controls intended to restrict access to data and systems, as well as other information security controls continue to threaten the confidentiality and availability of its financial and tax processing systems and information, and limit assurance of the integrity and reliability of its financial and taxpayer information. Unresolved, previously reported weaknesses and newly identified ones increase the risk of unauthorized disclosure, modification, or destruction of financial and sensitive taxpayer information.

IRS Did Not Sufficiently Control Access to Information Resources

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Inadequate access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service. Access controls include those related to user identification and authentication, authorization, cryptography, audit and monitoring, and physical security. IRS did not ensure that it consistently implemented effective access controls in each of these areas, as the following sections in this report demonstrate.

Controls for Identifying and Authenticating Users Were Not Consistently Enforced

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system also must establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. The combination of identification and authentication—such as user account/password combinations—provides the basis for establishing individual accountability and for controlling access to the system. The *Internal Revenue Manual* requires IRS to enforce strong passwords for authentication (defined as a minimum of eight characters, containing at least one numeric or special character, and a mixture of at least one uppercase and one lower case letter). In addition, IRS policy states that user accounts should be removed from the system or application if users have not logged on in 90 days. Furthermore, the *Internal Revenue Manual* requires that passwords be protected from unauthorized disclosure when stored.

IRS did not always enforce strong password management on systems at the three sites reviewed. For example, several user account passwords on UNIX systems did not meet password length or complexity requirements. Allowing weak passwords increases the likelihood that passwords will be compromised and used by unauthorized individuals to gain access to sensitive IRS information. In addition, user accounts for servers supporting the administrative accounting system had not been used in approximately 180 days, but still remained active at all three sites. Allowing inactive user accounts to remain on the system increases the likelihood of unauthorized individuals using these dormant accounts to

Users Were Routinely Given
More System Access Than
Needed to Perform Their Jobs

gain access to sensitive IRS data. Further, password and associated user IDs were stored in clear text on an intranet Web site which was accessible by unauthenticated users. As a result, individuals accessing this Web site could view these passwords and use them to gain unauthorized access to IRS systems. Such access could be used to alter data flowing to and from the agency's administrative accounting system.

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic principle for securing computer resources and information. This principle means that users are granted only those access rights and permissions they need to perform their official duties. To restrict legitimate users' access to only those programs and files they need to do their work, organizations establish access rights and permissions. "User rights" are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that regulate which users can access a particular file or directory and the extent of that access. To avoid unintentionally authorizing users' access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions. IRS policy states that the configuration and use of system utilities are based on least privilege and are limited to those individuals that require them to perform their assigned functions.

IRS permitted excessive access to systems by granting rights and permissions that gave users more access than they needed to perform their assigned functions. For example, one data center allowed all mainframe users access to powerful system management functions including storage management and mainframe hardware configurations. In addition, the center did not tightly restrict the ability to modify mainframe operating system configurations. Approximately 60 persons had access to commands that could allow them to make significant changes to the operating system, increasing the risk of inadvertent or deliberate disruption of system operations. Furthermore, IRS did not properly restrict file permission privileges. Excessive file privileges were given to an administrative accounting subsystem's file transfer account. As a result, any user with access to accounts on this server could gain unauthorized access to other servers within the administrative accounting system infrastructure.

Sensitive Data Were Not Always Encrypted

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption. Encryption can be used to provide basic data confidentiality and integrity by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. IRS policy requires the use of encryption for transferring sensitive but unclassified information between IRS facilities. The National Security Agency also recommends disabling protocols that do not encrypt information, such as user ID and password combinations, transmitted across the network.

IRS did not always ensure that sensitive data were protected by encryption. Although IRS had an initiative underway to encrypt its laptops, certain data were not encrypted. For example, at two data centers, administrator access to a key IRS application contained unencrypted data logins. These unencrypted logins could reveal usernames, passwords, and other credentials. By not encrypting data, IRS is at increased risk that an unauthorized individual could gain unwarranted access to its systems and/or sensitive information.

Logging Procedures Did Not Effectively Capture Changes to Mainframe Datasets

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail—logs of system activity—that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security-relevant events. IRS policy requires that audit records be created, protected, and retained to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

Although IRS had implemented logging capabilities for the servers reviewed, it did not effectively capture changes to datasets on the mainframe, which supports the agency's general ledger for tax administration. Specifically, it did not configure its security software to log successful changes to datasets that contain parameters and procedures on the mainframe used to support production operations of the operating system, system utilities, and user applications. By not recording changes to these datasets, IRS is at increased risk that unapproved or inadvertent

Weaknesses in Physical Security Controls Reduced Their Effectiveness

changes that compromise security controls or disrupt operations are made and not detected.

Physical security controls are essential for protecting computer facilities and resources from vandalism and sabotage, theft, accidental or deliberate destruction, and unauthorized access and use. Physical security controls should prevent, limit, and detect access to facility grounds, buildings, and sensitive work areas and the agency should periodically review the access granted to computer facilities and resources to ensure this access is still appropriate. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, and locks. The absence of adequate physical security protections could lead to the loss of life and property, the disruption of functions and services, and the unauthorized disclosure of documents and information. NIST requires that designated officials within the organization review and approve the access list and authorization credentials. Similarly, IRS policy requires that branch chiefs validate the need of individuals to access a restricted area based on authorized access lists, which are prepared monthly. To further address physical security, the *Internal Revenue Manual* requires periodic review of all mechanical key records.

Although IRS has implemented physical security controls, certain weaknesses reduce the effectiveness of these controls in protecting and controlling physical access to assets at IRS facilities, such as the following:

- One data center allowed at least 17 individuals access to sensitive areas without justifying a need based on their job duties.
- The same data center did not always remove physical access authorizations into sensitive areas in a timely manner for employees who no longer needed it to perform their jobs. For example, a manager reviewed an access listing dated March 2007 and identified 54 employees whose access was to be removed; however, at the time of our site visit in June 2007, 29 of the 54 employees still had access.
- Another data center did not perform monthly reviews of an authorized access list to verify that employees continued to warrant access to secure computing areas; according to agency officials, they perform a biannual review every 6 months or whenever a change occurs instead.
- The same data center also did not perform a periodic review of records accounting for mechanical keys used to gain access to sensitive areas.

As a result, IRS is at increased risk of unauthorized access to, and disclosure of, financial and taxpayer information, inadvertent or deliberate disruption of services, and destruction or loss of computer resources.

Weaknesses in Other Information Security Controls Increased Risk

In addition to access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an organization's information. These controls include policies, procedures, and techniques for securely configuring information systems and segregating incompatible duties. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of IRS's information and information systems.

Configuration Management Policies Were Not Fully Implemented

The purpose of configuration management is to establish and maintain the integrity of an organization's work products. Organizations can better ensure that only authorized applications and programs are placed into operation by establishing and maintaining baseline configurations and monitoring changes to these configurations. According to IRS policy, changes to baseline configurations should be monitored and controlled. Patch management, a component of configuration management, is an important factor in mitigating software vulnerability risks. Up-to-date patch installation can help diminish vulnerabilities associated with flaws in software code. Attackers often exploit these flaws to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations' systems. According to NIST, the practice of tracking patches allows organizations to identify which patches are installed on a system and provides confirmation that the appropriate patches have been applied. IRS's patch management policy also requires that patches be implemented in a timely manner and that critical patches are applied within 72 hours to minimize vulnerabilities.

IRS did not always effectively implement configuration management policies. For example, one data center did not ensure that its change control system properly enforced change controls to two key applications residing on the mainframe. The current configuration could allow individuals to make changes without being logged by the agency's automated configuration management system. Furthermore, servers at these locations did not have critical patches installed in a timely manner. For example, at the time of our site visit in July 2007, one site had not installed critical patches released in February 2007 on two servers. As a result, IRS has limited assurance that only authorized changes are being made to its systems and that they are protected against new vulnerabilities.

Incompatible Duties Were Not Always Appropriately Segregated

Segregation of duties refers to the policies, procedures, and organizational structures that help ensure that no individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often, organizations segregate duties by dividing responsibilities among two or more individuals or organizational groups. This diminishes the likelihood that errors and wrongful acts will go undetected, because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. The *Internal Revenue Manual* requires that IRS divide and separate duties and responsibilities of incompatible functions among different individuals, so that no individual shall have all of the necessary authority and system access to disrupt or corrupt a critical security process.

IRS did not always properly segregate incompatible duties. For example, mainframe system administration functions were not appropriately segregated. IRS configured a user group that granted access to a broad range of system functions beyond the scope of any single administrator's job duties. Granting this type of access to individuals who do not require it to perform their official duties increases the risk that sensitive information or programs could be improperly modified, disclosed, or deleted. In addition, at one data center, physical security staff who set user proximity card access to sensitive areas were also allowed to determine whether employees needed access or not, rather than leaving the decision to cognizant managers. As a result, staff could be allowed improper access to sensitive areas.

IRS Has Not Fully Implemented Its Information Security Program

A key reason for the information security weaknesses in IRS's financial and tax processing systems is that it has not yet fully implemented its agencywide information security program to ensure that controls are effectively established and maintained. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;

-
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce risks, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
 - plans for providing adequate information security for networks, facilities, and systems;
 - security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
 - periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that include testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
 - a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security policies, procedures, or practices; and
 - plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Although IRS continued to make important progress in developing and documenting a framework for its information security program, key components of the program had not been fully or consistently implemented.

Although a Risk Assessment Process Was Implemented, Potential Risks Were Not Always Assessed

According to NIST, risk is determined by identifying potential threats to the organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data. Identifying and assessing information security risks are essential to determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that these policies and controls operate as intended. OMB *Circular A-130*, appendix III prescribes that risk be reassessed when significant changes are made to computerized systems—or at least every 3 years. Consistent with NIST guidance, IRS requires its risk assessment

process to detail the residual risk assessed and potential threats, and to recommend corrective actions for reducing or eliminating the vulnerabilities identified.

Although IRS had implemented a risk assessment process, it did not always effectively evaluate potential risks for the systems we reviewed. The six risk assessments that we reviewed were current, documented residual risk assessed and potential threats, and recommended corrective actions for reducing or eliminating the vulnerabilities they identified. However, IRS did not identify many of the vulnerabilities that we identify in this report and did not assess the risks associated with them. As a result, potential risks to these systems may be unknown. We have previously identified this weakness and recommended that the agency update its risk assessments to include vulnerabilities we identified. IRS is in the process of taking corrective action.

Although IRS Policies and Procedures Were Generally Adequate, Guidance for Logging Mainframe Activity Was Unclear

Another key element of an effective information security program is to develop, document, and implement risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. If properly implemented, policies and procedures should help reduce the risk that could come from unauthorized access or disruption of services. Technical security standards provide consistent implementation guidance for each computing environment. Developing, documenting, and implementing security policies are the important primary mechanisms by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls. In addition, agencies need to take the actions necessary to effectively implement or execute these procedures and controls. Otherwise, agency systems and information will not receive the protection that the security policies and controls should provide.

IRS has developed and documented information security policies, standards, and guidelines that generally provide appropriate guidance to personnel responsible for securing information and information systems; however, guidance for securing mainframe systems was not always clear. For example, the *Internal Revenue Manual* does not always specify when successful system changes should be logged. Further, although IRS policy provides general requirements for protection of audit logs, the manual for mainframe security software does not provide detailed guidance on what logs to protect and how to protect them. As a result, IRS has reduced assurance that these system changes are being captured and that its systems and the information they contain, including audit logs, are being sufficiently protected.

Security Plans Adequately Documented Management, Operational, and Technical Controls

An objective of system security planning is to improve the protection of information technology resources. A system security plan provides an overview of the system's security requirements and describes the controls that are in place or planned to meet those requirements. OMB *Circular A-130* requires that agencies develop system security plans for major applications and general support systems, and that these plans address policies and procedures for providing management, operational, and technical controls. Furthermore, IRS policy requires that security plans describing the security controls in place or planned for its information systems be developed, documented, implemented, reviewed annually, and updated a minimum of every 3 years or whenever there is a significant change to the system.

The six security plans we reviewed documented the management, operational, and technical controls in place at the time the plans were written, and the more recent plans mapped those controls directly to controls prescribed by NIST. According to IRS officials, at the time of our review, they were in the process of updating two of these plans to more accurately reflect the current operating environment. The remaining four plans appropriately reflected the current operating environment.

Although Training Was Provided, Employees with Significant Security Responsibilities at One Center Did Not Receive the Needed Training

People are one of the weakest links in attempts to secure systems and networks. Therefore, an important component of an information security program is providing required training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks. IRS policy requires that personnel performing information technology security duties meet minimum continuing professional education hours in accordance with their roles. Personnel performing technical security roles are required by IRS to have 12, 8, or 4 hours of specialized training per year, depending on their specific role.

Although IRS has made progress in providing security personnel with a job-related training curriculum, IRS did not ensure that all employees with significant security responsibilities received adequate training. For example, based on the documentation we reviewed, all 40 employees selected at one data center met the required minimum training hours; however, 6 of 10¹⁰ employees reviewed at another center did not.

¹⁰Based on documentation provided, of the 10 employees we reviewed, 3 employees met the required minimum training hours and 6 did not. IRS notified us that the remaining employee had separated from the agency.

According to IRS officials, these six employees with significant security responsibilities were not identified by their managers for the required training. Until managers identify individuals requiring specialized training, IRS is at increased risk that individuals will not receive the training necessary to perform their security-related responsibilities.

Although Controls Were Tested and Evaluated, Tests Were Not Always Comprehensive

Another key element of an information security program is to test and evaluate policies, procedures, and controls to determine whether they are effective and operating as intended. This type of oversight is a fundamental element because it demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results improve the security program. FISMA requires that the frequency of tests and evaluations be based on risks and occur no less than annually. IRS policy also requires periodic testing and evaluation of the effectiveness of information security policies and procedures, as well as reviews to ensure that the security requirements in its contracts are implemented and enforced.

IRS tested and evaluated information security controls for each of the systems we reviewed. The more current tests and evaluations had detailed methodologies, followed NIST guidance, and documented the effectiveness of the tested controls. However, the scopes of these tests were not sufficiently comprehensive to identify significant vulnerabilities. For example, although IRS and GAO examined controls over the same systems, we identified unencrypted passwords on an internal Web site that IRS had not. Our test results also showed that contractors did not always follow agency security policies and procedures. To illustrate, contractors had inappropriately stored clear-text passwords and sensitive documents on internal agency Web sites. Although IRS had numerous procedures to provide contractor oversight, it had not detected its contractors' noncompliance with its policies. Because IRS had not identified these weaknesses, it has limited assurance that appropriate controls were being effectively implemented.

Remedial Action Plans Were Not Always Complete, and Corrective Actions Were Not Effective

A remedial action plan is a key component described in FISMA. Such a plan assists agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses that are found in information systems. In its annual FISMA guidance to agencies, OMB requires agencies' remedial action plans, also known as plans of action and milestones, to include the resources necessary to correct an identified

weaknesses. According to IRS policy, the agency should document weaknesses found during security assessments as well as document any planned, implemented, and evaluated remedial actions to correct any deficiencies. The policy further requires that IRS track the status of resolution of all weaknesses and verify that each weakness is corrected.

IRS has developed and implemented a remedial action process to address deficiencies in its information security policies, procedures, and practices. However, this remedial action process was not working as intended. For example, IRS had identified weaknesses but did not always identify necessary resources to fix them. Specifically, we reviewed remedial action plans for five of the six systems¹¹ and found that plans for four of them had not identified what, if any, resources were necessary to support the corrective actions. Subsequent to our site visits, IRS provided additional information on resources to support corrective actions for three of them.

In addition, the verification process used to determine whether remedial actions were implemented was not always effective. IRS indicated that it had corrected or mitigated 39 of the 98 previously reported weaknesses. However, of those 39 weaknesses, 10 still existed at the time of our review. Furthermore, one facility had actually corrected less than half of the weaknesses reported as being resolved. We have previously identified a similar weakness and recommended that IRS implement a revised remedial action verification process that ensures actions are fully implemented, but the condition continued to exist at the time of our review. Without a sound remediation process, IRS will not have assurance that the proper resources will be applied to known vulnerabilities or that those vulnerabilities will be properly mitigated.

Contingency Plans Were Not Always Complete or Tested

Continuity of operations planning, which includes contingency planning, is a critical component of information protection. To ensure that mission-critical operations continue, it is necessary to be able to detect, mitigate, and recover from service disruptions while preserving access to vital information. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. In addition, testing contingency plans is essential to determine whether the plans will function as intended in an emergency situation. FISMA requires that agencywide information security programs include

¹¹Based on IRS documentation, one of the systems did not require that a remedial action be developed.

plans and procedures to ensure continuity of operations. IRS contingency planning policy requires that essential IRS business processes be identified and that contingency plans be tested at least annually.

Although the systems reviewed had contingency plans, the plans were not always complete or tested. For example, for three of the six plans, IRS had not identified essential business processes. Further, the agency had not annually tested two of the plans, which were both dated September 2005. IRS informed us that these issues will be addressed during current certifications and accreditations for those systems. However, until IRS identifies these essential processes and sufficiently tests the plans, increased risk exists that it will not be able to effectively recover and continue operations when an emergency occurs.

Conclusions

IRS has made only limited progress in correcting or mitigating previously reported weaknesses, implementing controls over key financial systems, and developing and documenting a framework for its agencywide information security program. Information security weaknesses—both old and new—continue to impair the agency’s ability to ensure the confidentiality, integrity, and availability of financial and taxpayer information. These deficiencies represent a material weakness in IRS’s internal controls over its financial and tax processing systems. A key reason for these weaknesses is that the agency has not yet fully implemented critical elements of its agencywide information security program. The financial and taxpayer information on IRS systems will remain particularly vulnerable to insider threats until the agency (1) fully implements a comprehensive agencywide information security program that includes enhanced policies and procedures, appropriate specialized training, comprehensive tests and evaluations, sufficient contractor oversight, updated remedial action plans, and a complete continuity of operations process; and (2) begins to address weaknesses across the service, its facilities, and computing resources. As a result, financial and taxpayer information is at increased risk of unauthorized disclosure, modification, or destruction, and IRS management decisions may be based on unreliable or inaccurate financial information.

Recommendations for Executive Action

To help establish effective information security over key financial processing systems, we recommend that you take the following seven actions to implement an agencywide information security program:

- Update policies and procedures for configuring mainframe operations to ensure they provide the necessary detail for controlling and logging changes.
- Identify individuals with significant security responsibilities to ensure they receive specialized training.
- Expand scope for testing and evaluating controls to ensure more comprehensive testing.
- Enhance contractor oversight to better ensure that contractors' noncompliance with IRS information security policies is detected.
- Update remedial action plans to ensure that they include what, if any, resources are required to implement corrective actions.
- Identify and prioritize critical IRS business processes as part of contingency planning.
- Test contingency plans at least annually.

We are also making 46 detailed recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct specific information security weaknesses related to user identification and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, and segregation of duties.

Agency Comments

In providing written comments (reprinted in app. I) on a draft of this report, the Acting Commissioner of Internal Revenue agreed that IRS has not yet fully implemented critical elements of its agencywide information security program, and stated that the security and privacy of taxpayer information is of great concern to the agency. She recognized that there is significant work to be accomplished to address IRS's information security deficiencies, and stated that the agency is taking aggressive steps to correct previously reported weaknesses and improve its overall information security program. She also noted that IRS has taken many actions to strengthen its information security program, such as installing

automatic disk encryption on its total deployed inventory of approximately 52,000 laptops, and creating a team of security and computer experts to improve mainframe controls. Further, she stated that the agency is committed to securing its computer environment, and will develop a detailed corrective action plan addressing each of our recommendations.

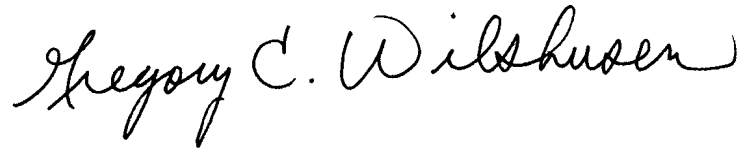
This report contains recommendations to you. As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform not later than 60 days from the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report. Because agency personnel serve as the primary source of information on the status of recommendations, GAO requests that the agency also provide it with a copy of your agency's statement of action to serve as preliminary information on the status of open recommendations.

We are sending copies of this report to interested congressional committees and the Secretary of the Treasury. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you have any questions regarding this report, please contact Gregory Wilshusen at (202) 512-6244 or Nancy Kingsbury at (202) 512-2700.

We can also be reached by e-mail at wilshuseng@gao.gov and kingsburyn@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Sincerely yours,

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, prominent "G" and "W".

Gregory C. Wilshusen
Director, Information Security Issues

A handwritten signature in black ink that reads "Nancy R. Kingsbury". The signature is written in a cursive style with a large, prominent "N" and "K".

Nancy R. Kingsbury
Managing Director, Applied Research and Methods

Appendix I: Comments from the Internal Revenue Service



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

December 14, 2007

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report, *Information Security: IRS Needs to Address Pervasive Weaknesses (GAO-08-211, Public version)*. While we agree that we have not yet fully implemented critical elements of our agency-wide information security program, the security and privacy of taxpayer information is of great concern to the IRS. We recognize that there is significant work to be accomplished to address our information security deficiencies, and we are taking aggressive steps to correct previously reported weaknesses and improve our overall information security program.

We will review all of the corrective actions the GAO previously reported to ensure that our actions include sustainable fixes that fully resolve the weaknesses. We will provide the detailed corrective action plan addressing each of the recommendations with our response to the final report.

We do appreciate that your draft report recognizes that the IRS has made some progress in improving its information security program and has numerous initiatives underway. Even throughout this audit process the IRS team worked proactively with your staff to identify solutions to the issues your staff raised. In fact, this support provided by your GAO technical team enabled us to implement a number of fixes even as this audit report was being prepared, which was most helpful.

In 2007, we took many actions to strengthen the IRS information security program, some of which you acknowledged in your draft report:

- Completed required Federal Information Security Management Act annual activities, including security testing on 260 applications and systems
- Installed automatic disk encryption on the total deployed inventory of IRS laptops (approximately 52,000)

2

- Implemented a data encryption solution for mainframe tapes exchanged with federal, state, and other partners
- Issued cable locks for all employees with laptops, to improve physical security
- Created a special team reflecting a partnership of security and computer experts to improve mainframe controls, including controls for access privileges, and scheduler and dataset changes
- Implemented a Two-Factor authentication for remote access to IRS networks by adding a physical password grid card in addition to the standard user name and password
- Implemented an enterprise anti-virus Internet gateway solution to detect and quarantine malicious content from invading systems
- Established a Security Services and Privacy Executive Steering Committee to provide oversight over the corrective action plans and initiatives to improve the security posture of the IRS
- Established a new executive position reporting directly to the IRS Deputy Commissioner that is focused on taxpayer privacy and identity theft
- Implemented a comprehensive communications strategy to educate employees on data protection responsibilities and the use of encryption tools

In FY 2008, the performance agreements of all IRS executives will include a specific performance standard focused on resolving security weaknesses and reporting the security compliance status of all computer systems connected to the IRS network. Also, the IRS has obtained additional expert-level technical support to assist in the development of a comprehensive security analysis of the architecture, processes, and operations of the mainframe computing center complex in order to develop a roadmap and strategy to address several of the issues noted by GAO in the report.

In closing, we want to reiterate that we fully appreciate the seriousness of these deficiencies and are committed to securing our computer environment, as we re-evaluate current processes, promote user awareness, and apply innovative ideas to increase compliance. We appreciate your continued support and guidance as we work to correct our deficiencies, and we look forward to working with you further to develop appropriate measures. If you have any questions or would like to discuss our response in further detail, please contact Arthur Gonzalez, Chief Information Officer, at 202-622-6800.

Sincerely,



Linda E. Stiff
Acting Commissioner of Internal Revenue

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov
Nancy R. Kingsbury, (202) 512-2700 or kingsburyn@gao.gov

Staff Acknowledgments

In addition to the persons named above, Gerard Aflague, Bruce Cain, Larry Crosland, Mark Canter, Denise Fitzpatrick, David Hayes (Assistant Director), Nicole Jarvis, Jeffrey Knott (Assistant Director), George Kovachick, Kevin Metcalfe, Eugene Stevens, and Amos Tevelow made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, jarmong@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548